STRATEGY RESEARCH PROJECT



# IMPLICATIONS OF OUTSOURCING ON NETWORK CENTRIC WARFARE

BY

LIEUTENANT COLONEL MICHAEL A. BROWN
United States Army



USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

# Implications of Outsourcing on Network Centric Warfare

by

Lieutenant Colonel Michael A. Brown
United States Army

Professor Kevin Cogan
Project Advisor



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: LTC Michael A. Brown

TITLE: Implications of Outsourcing on Network Centric Warfare

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 31 CLASSIFICATION: Unclassified

The Department of Defense (DOD) has taken about 80 percent of the government cutbacks since the end of the Cold War. As a means to fashion cost savings and gain efficiencies, DOD is seeking to streamline much of its infrastructure. One popular idea to assist in the streamlining effort is through the outsourcing of Information Technology (IT) functions. There is a sentiment within the Department of the Army (DA) that the entire Information Management/Information Systems element of the Army can be outsourced without having an impact to the Army. The purpose of this research paper is to examine this sentiment to determine if it makes sense or where it could create problems as the Army moves towards a network centric warfare environment. It will examine the Army's IT requirements to support network centric warfare, examine potential outsourcing options, and determine the implications of these options to the effectiveness of achieving the requirements.

TABLE OF CONTENTS

## IMPLICATIONS OF OUTSOURCING ON NETWORK CENTRIC WARFARE

The Department of Defense (DOD) has taken about 80 percent of the government cutbacks since the end of the Cold War resulting in the loss of approximately 355,000 civilian and 743,000 military jobs. Even with these heavy cuts in the workforce, DOD has still failed to generate enough savings to offset planned procurements. To fashion additional cost savings and gain efficiencies, DOD is seeking additional ways to improve its modernization and procurement spending on "core" competencies. One popular idea to assist in the streamlining effort is through the outsourcing of Information Technology (IT) functions.[1]

There are already examples within DOD where this trend is occurring. In August 2001, the National Security Agency (NSA) awarded a 10-year contract to Computer Sciences Corp. This contract will provide unclassified computing and telecommunications services to the NSA as well as the designing and maintaining of classified systems used for the management of electronic signals and digital data intercepted around the globe.[2]

The Department of the Navy is preparing to outsource the vast portion of its unclassified information systems and technology infrastructure through a program called the Navy Marine Corps Intranet (NMCI). The NMCI is a corporate-style intranet that will link together Navy and Marine Corps installations. The program is designed to allow 350,00 Navy and 68,000 Marine Corps users to exchange data, voice, and video communications from their desktops anywhere around the world. While the network and systems in NMCI are not new, what is new is the concept of outsourcing the management, maintenance and upgrades of the network, software procurement and upgrades, and life cycle computer replacement. These functions have been contracted out to Electronic Data Systems Corporation. Rough estimates place the annual cost of outsourcing the NMCI at about $2 billion a year, or $10 billion over the life of the five-year contract, saving the Navy an estimated 28% on current IT costs.[3]

Seeing this trend and the potential savings, there is a growing sentiment within the Department of the Army (DA) that the Army can maximize savings and efficiencies through the outsourcing of its Information Management/Information Systems throughout the force. While the cost saving potential is feasible, what has not been determined is what are the implications to the warfighter and national security as we move toward the realm of network centric warfare.

Today and tomorrow our national security depends upon Information Technology. The Army cannot move a Corps against a 21st century adversary, communicate battlefield information, deliver supplies, assign personnel or perform a thousand other functions without Information Technology. As the Army transforms from a legacy force to an objective force, from

now until about the year 2020, the interim force must maintain its ability to fight and win our nation's wars. The decisions the Army makes today will affect the force of tomorrow. So what are the implications to the interim force and network centric warfare (NCW) if the Army decides to outsource IT functions for the sake of conserving fiscal resources? To understand the implications we must first understand the concept of network centric warfare and the Army's contributions and support requirements during this transitional period. Once this is understood we can then examine outsourcing options and their implications to the warfighter, the warfighting mission and the Army. From this analysis we can then determine the best courses of action to meet the goal of network centric warfare without sacrificing our nation's security.

**NETWORK CENTRIC WARFARE**

Joint Vision 2020 (JV 2020) states that the US military must be a joint force capable of full spectrum dominance. This transformation is achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. One key enabler of full spectrum dominance is our ability to gain information superiority. Information superiority may be defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[4] To gain information superiority requires a concept to achieve this vision. Network centric warfare is this concept.

Network centric warfare is a concept about means. To operate in a network centric environment is not an objective or a goal of combat. Rather, network centric warfare is a tool, a means to empower military operations to accomplish strategic objectives, or ends. Networked centric operations are military operations that are enabled by the electronic networking of the force. They are joint and combined operations. The networks—and their employment—do not acknowledge sea, land, or air. The networks operate as one. When these operations take place in the context of warfare, the term network centric warfare is applicable.

Given this broad concept, network centric warfare may then be defined as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledge entities in the battlespace.[5] The basic principles of warfare will not change; however, commanders will apply those principles at previously unachievable levels and with previously unachievable speed because they will have a

comprehensive information picture of the battlespace. The focus of warfare will go from trying to gather information in order to develop a course of action to applying information to effect outcomes of battles and campaigns. NCW relieves the commander from the task of amassing information. It is provided for them. NCW will eliminate cumbersome steps previously required to arrive at the point where a decision can be made and allow that time and energy to be funneled into assessment and decision making.[6]

Imagine, if you will, the following example. A tactical unmanned aerial vehicle locates an enemy artillery battery setting up to fire against friendly forces. This information is immediately seen at the commander's tactical operations center. The commander, through network analysis nodes, is also provided with the weapon type, range and accessible targets within range of the enemy battery. Simultaneously, with this information the commander is also provided with information on all friendly weapon systems (land, sea or air) that are capable of interdicting the enemy guns. The commander decides the best weapon to employ based on his friendly situational picture information (probability of kill, weapon maintenance status, ammunition supply, etc..) which is also instantaneously provided. A fire mission is sent and executed by the appropriate weapon system via the command and control system and the target is destroyed. What under today's methodology would take many minutes to hours to execute, can now be accomplished in seconds with greater effect. A networked force can make this a reality and NCW is the tool that will transform the way we plan and fight.

The key to NCW and this transformation is the capability to effectively network the sensors, decision-makers and the shooters. Taken together the sensor grid, the command and control or information grid, and the engagement or shooter grid combine to enable rapid, precise offensive and defensive action.[7] The network is a combination of these grids and is referred to as the Global Information Grid (GIG). The Global Information Grid is the backbone of NCW and is the unifying theme that will provide warfighters with secure global access to information. The GIG is the enabler of NCW and the key to information superiority.

## THE GLOBAL INFORMATION GRID

The DOD Chief Information Officer defines the GIG as follows:

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all

> Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, Allied, and non-DOD users and systems.[8]

In simple terms, the Global Information Grid provides the right information at the right time in the right format to the right warfighter. The Global Information Grid will play the key role in networking the force and extending and securing the warfighters' information domain to enable network centric warfare and information superiority. To achieve information superiority through the GIG, the GIG must be dynamic and adaptable to changes in the operational environment, flexible and secure. The GIG must provide end-to-end visibility, control, and support to manage and protect networks and the information they carry. To provide these functions, the GIG is highly dependent on information management/information system (IT/IS) capabilities.

To provide these capabilities the GIG focuses on seven components: the Warrior, Global Applications, Communications, Computing, Network Operations, Information Management, and Foundation components.[9] The combination and application of these seven components is what will make the GIG and Network Centric Warfare a reality. But for the US military to realize the full potential of network centric warfare, each service must contribute to the effort. Each service of the military is responsible for providing the service unique system functionality required to support their service and the components to the GIG .

**ARMY CONTRIBUTIONS TO NCW AND THE GIG**

To support JV 2020 and NCW, the Army is transforming. The Army envisions a strategically responsive force that is dominant across the entire spectrum of operations and is responsive, deployable, agile, versatile, lethal, survivable, and sustainable. The goal is to have a force that can deploy and sustain a brigade in 96 hours, a division in 120 hours and five divisions in 30 days, anywhere in the world.[10] To achieve this vision, the Army has implemented a strategy of evolution from our current legacy force to a force of the future called the objective force. To support this transition the Army is not only procuring new weapons technologies but they are developing and deploying the enabling architecture, programs and services required to network our forces and installations. The Army's programs and initiatives are rooted in digitization and are vectored to support NCW concepts and the GIG. The Army's efforts to move toward NCW can be seen by highlighting (though not inclusive of all) the systems and services provided for each component of the GIG.

THE WARRIOR COMPONENT:

The warrior component is the decision maker-sensor-shooter structure that enables battlefield situational awareness and operational execution. This component supplies information on demand through "plug and play" systems. The systems within the warrior component are generally being planned for Corps and below type units. The Army is investing heavily in this component to improve its warfighting capability. Examples of the systems that are being developed and deployed by the Army that would fall into this component are:[11]

– The Maneuver Control System (MCS): MCS is the primary battle command information system and is in effect, the Commander's computer. It serves as the horizontal and vertical integrator of force level sensor to shooter information at battalion through corps level.

- The Advanced Field Artillery Tactical Data System (AFATDS): AFATDS is an automated Fire Support C2 system. It provides automated support for planning, coordination, control and execution of close support, counterfire, interdiction and air defense suppression fires.

– The All Source Analysis System (ASAS): ASAS serves as the ground commander's (from Echelon Above Corps down to battalion) all source central intelligence processor for compartmented and collateral information received from intelligence collection systems, sensors and front-line soldiers and for information accessed from service, joint and national databases.

– Force XXI Battle Command Brigade and Below (FBCB2): FBCB2 provides near real-time situational awareness to individual weapons, tactical vehicles and Tactical Operations Centers (TOCs). FBCB2 generates position location reports and equipment status and distributes them to friendly forces throughout the battlefield.

– The Air and Missile Defense Work Station (AMDWS): AMDWS is a common air/missile defense planning, situational awareness, and staff planning tool that will integrate all echelons of command air/missile defense weapon systems throughout the Air Defense Artillery force structure on the battlefield.

– The Combat Service Support Control System (CSSCS): CSSCS is the commander's logistical command and control system. It allows for rapid collection, storage, analysis, and dissemination of critical logistics, medical, financial, and personnel information.

THE GLOBAL APPLICATIONS COMPONENT

The global applications component is a comprehensive worldwide capability to provide leaders a global common operating picture. It consists of those systems that link the warrior component to the higher level assets to enable ground force commanders, joint force

commanders and national leaders to maintain a common global operating picture. They range from business applications and electronic commerce through intelligence systems. Currently there are over 28,000 systems throughout the Department of Defense that would fall into this component. Examples of Army systems that would fit into this component are:[12]

– The Global Command and Control System-Army (GCCS-A): GCCS-A is the Army link to the Joint GCCS and is the means by which the Army and Joint forces share the Common Operating Picture (COP).

– The Global Combat Support System-Army (GCSS-A): GCSS-A is the Army link to the joint logistical command and control system. GCSS-A folds the CSSCS functionality into the global component for world-wide dissemination.

– The Digitized Topographic Support System (DTSS): DTSS provides commanders at all levels with digital and hardcopy geospatial products. DTSS accepts topographic and multispectral imagery data from NIMA, commercial sources, and National Technical Means assets to provide the commander with the foundation for the COP.

– The Integrated Meteorological System (IMETS): IMETS provides the commander at all levels with an automated weather system that receives, processes and disseminates weather information from the Air Force Weather Agency and meteorological sensor inputs.

THE COMMUNICATIONS COMPONENT

The communications component is the transport grid that extends from post, camps, and stations through the strategic networks to the "last tactical mile." The last tactical mile being the weapon or sensor platform. For the Army, this component can be subdivided into two categories, strategic communications and tactical communications. Tactical communications consists of all assets assigned to Echelon Above Corps Signal Battalions through individual Battalion level assets. It includes assets such as the Single Channel Ground and Airborne Radio System (SINCGARS), the Mobile Subscriber Equipment (MSE) System, the Tri-Service Tactical Communications (TRI-TAC) System, Military and Commercial Satellite Systems, Fiber Optic Systems and Wireless Communication systems. The communication component is vital to the success of NCW warfare by insuring the data required by the warrior and global components reach the proper location in a timely manor. The goal of this component is to provide information and bandwidth on demand. The following are examples of the effort being taken by the Army to improve this component.[13]

– The Tactical High-Speed Data Network (THSDN): THSDN is the interim answer that provides a moderate increase in data throughput to support the warrior component needs for

passing data. The THSDN will be fielded to Army MSE and TRI-TAC Signal Battalions. The THSDN will provide the warrior the capability to network the assets from the warrior component and the global component.

– The High Capacity Line-of-Sight (HCLOS) Radio: The HCLOS radio provides increased data transmission capabilities to support Line-of-Sight communications within MSE and TRI-TAC Signal Battalions. The HCLOS radio increases throughput from 256 KBs to 2 MBs on extension links and from 1048 KBs to 8 MBs on the backbone trunks.

– The Warfighter Information Network-Tactical (WIN-T): WIN-T will use military and commercial technology to move information around the battlefield as well as between the sustaining base and the deployed warfighter. WIN-T integrates communication platforms from the strategic level to the tactical level. It will be the system that replaces MSE and TRI-TAC Systems.

– The Installation Information Infrastructure Modernization Program (I3MP): I3MP is the key initiative to upgrade and digitize the information infrastructure at Army installations. The upgrade provides the connectivity internal to the installation and external to other Active Continental United States support activities and to deployed combat forces. These upgrades are essential to the entire digitization process because they provide linkages to deployed forces, enable split based operations, and provide connectivity from every installation into GCCS-A and GCSS-A. There are four major components to the program. The Outside Cable Rehabilitation component will install a high capacity fiber network backbone on our installations. The Common User Installation Transport Network will provide the "branch networks" off the main fiber backbone. The Army DISN Router Program will link the installations into the Army networks and the MACOM Telephone Modernization Program will provide modern digital telephone systems to the installations. These programs will provide a single solution for data and data fusion requirements (data, voice, video), and computer network support.[14]

## THE COMPUTING COMPONENT

The computing component consists of hardware, software, and processing functions that, like the communications component, extends from the warrior component across the global applications component to provide uninterrupted distribution of information to all forces. The hardware, software, and data warehouses may be located within any element of the warrior or global applications component. The critical part of the computing component is the data connectivity required to share the information from data warehouse to user or from data warehouse to data warehouse. This aspect of the computing component is provided via the

Secret Internet Protocol Router Network (SIPRNET) and the Sensitive but Unclassified Internet Protocol Router Network (NIPRNET). These two networks are the backbone for all data traffic from installation down to the soldier on the battlefield. While there is emerging technology that will merge this two networks into one, the aspects of this component will remain the same.

## THE NETWORKING OPERATIONS COMPONENT

The network operations component is the management grid which provides an integrated and seamless end-to-end management of the grids, networks, applications and services across the GIG. This function is usually performed by signal personnel at the unit level and Signal Battalions at the strategic and tactical levels and Army Signal Command (ASC) at the Army level. At the tactical level, signal battalions and brigades serve as the system control element (SYSCON) from soldier to Corps level functions. Above Corps, the Theatre Signal Brigade provides a Theatre Network Operations and Security Center (TNOSC) and at Army level, ASC provides the Army Network Operations and Security Center (ANOSC). The function of these centers is to provide network management, information assurance, and configuration management services to any user of the GIG.

## THE INFORMATION MANAGEMENT COMPONENT

The information management component consists of those personnel and functions responsible for ensuring the users of the GIG and its components have the appropriate permissions and to access or input required data in the performance of their duties. Like the networking component, these functions may be performed from battalion level (signal soldiers) to the installation level by the Director of Information Management (DOIM) office.

## THE FOUNDATION COMPONENT

The foundation component consists of all the transforming activities that must happen involving people and organizations in order to make the GIG and NCW a reality. It is primarily a Training and Doctrine Command (TRADOC) and DA function. TRADOC, working with battle labs, operational units and DA, provides the transforming doctrinal changes, policy, and training in order to make NCW a reality.

To integrate, operate and manage the key IT components supporting the GIG requires an effective operational support system. These systems must include all elements necessary to maintain and operate all of the systems or networks associated with the components. The scope of this support varies among the components but generally includes maintenance,

system engineering, data management, configuration management and computer programming type skills. These are highly complex tasks that cannot be supported "on the fly." It requires specially trained and educated personnel for each function. Without properly trained and educated personnel, the GIG will surely fail. These personnel requirements can be generally divided into five basic categories. These categories are system operators, system administrators, network administrators, network managers and system engineers.

## SYSTEM OPERATORS

System operators are those personnel required to posses the technical skills and experience to operate the system by inputting data, retrieving data, provide an analysis of the data, and perform tasks associated with the system. Commonly referred to as the user, these personnel can be of any military occupational specialty (MOS) and belong to any unit whether it is combat arms, combat support or combat service support.

## SYSTEM ADMINISTRATORS

System Administrators are those personnel required to posses the technical skills and experience to manage a multi-user system. They must be familiar with Local Area Network (LAN) and Wide Area Network (WAN) applications. They are responsible for monitoring and managing routers, gateways, system servers, and remote access. They supervise, install, operate, and perform unit level maintenance on system servers and associated devices in mobile and fixed facilities. The system administrator can also be any MOS but is generally senior in rank to the system operator.

## NETWORK ADMINISTRATORS

Network administrators are those personnel required to posses the technical skills and experience to manage local and wide area networks. They perform network security functions, install new applications, distribute software upgrades, and monitor daily activities. They are responsible for managing routers, gateways, network servers and remote access. The network administrators are responsible for "plugging" any system within the components into the GIG to ensure proper functionality is achieved across the GIG.

## NETWORK MANAGERS

Network managers are those personnel capable of planning, directing and coordinating the activities throughout the GIG. They are responsible for the administration, program control and technical supervision of network and system administrators.

SYSTEM ENGINEERS

System engineers are those personnel who plan and provide the communications and data networks to insure internal and external connections between the systems and networks are accomplished.

When looking at all of the functions and complexities associated with the GIG there is no doubt that there is this requirement for these specialized personnel. But to dedicate and train personnel to support these functions detracts the Army from its core function – warfighting. Given the current policy of a "no growth" force, the more of these specialized personnel required to operate the systems means fewer warfighters available to prosecute our nations wars. So how does the Army do both?

**MEETING THE ARMY'S SKILL REQUIREMENTS – OUTSOURCING**

A means to fill the void between warfighting and system support requirements is through outsourcing. The term "outsourcing" refers to the use of external agents to perform one or more organizational activities. The Army's organizational success is determined by excellence in a small number of core competencies. Because these competencies are so crucial, the Army must maintain a preeminent operational capability in all of them. These core competencies are the warfighting skills required to prosecute our nation's wars. Skills required to support the core competencies are referred to as non-core competencies. The outsourcing of non-core competencies is an established commercial practice that is believed to lower costs and facilitate the acquisition of cutting-edge technology.

This is not a new or revolutionary thought in the Army. The Army has outsourced for many years, mostly in the area of "home-base" installation support functions. Only in recent years has the trend changed to outsourcing deployed forces and the trend is growing. In 1990 during the Gulf War, DA civilian and private or commercial contractors represented less than three percent of the total deployed force. In 1995 for Operation Enduring Freedom in Bosnia, the DA civilian and contractor work force deployed grew to nine percent.[15]

While an official Army policy or position on outsourcing IT competencies has not been made, there is a growing sentiment within DA that the Army can maximize savings and efficiencies by categorizing IT functions as non-core functions and outsource them. In 2001 the 4th Infantry Division deployed 275 IT contract personnel to support the division on a National Training Center rotation. If a plan or strategy is not developed, it is foreseeable that IT contractors will be located in every unit. But will this achieve the Army's intent?

The Army's goal for using and deploying contractors is to free up military manpower from combat support and combat service support type elements to focus on combat type units. The concept is that proper outsourcing will permit the Army to focus on its core competency – warfighting.[16] In terms of NCW, these non-core activities are those functions performed to support the GIG. This could range from system operator functions all the way to managing network operations required to support the GIG. But not only do these functions span the spectrum of NCW, they also encompass all Army units and locations. NCW will require these specialized personnel and functions to be preformed in every unit and installation within the Army. From battalions in Korea to the Chief of Staff of the Army in the Pentagon, NCW and the GIG will provide the Army a secure enabler to assist in the prosecution of its mission. But if the force structure is not able to expand to meet all the personnel requirements needed for NCW, what outsourcing options are available?

When considering outsourcing IT functions there are three basic options for the Army to consider:[17]

- Body shop outsourcing – This option is categorized as when management uses outsourcing as a way to meet short term demand. The most common type of body shop outsourcing is the use of contract personnel on a single system that is managed by the company employees. This type of outsourcing is currently seen throughout the Army as Project Managers and units hire contractors to install, operate and train military personnel on specific systems. These contractors are used as the system operators and system administrators of these systems. They are located within combat, combat support and combat service support units. They would accompany the unit on any deployment.
- Project management outsourcing – This option is categorized as when management outsources for a specific project or portion of IS work. Examples of project management outsourcing include the use of vendors to develop new systems, support existing applications, or manage a network. This type of outsourcing is currently seen throughout the Army as units hire contractors to manage their theater and Army data networks. The function of managing these networks is performed by the TNOSC's and the ANOSC. With the Chief of Staff of the Army's commitment to fill all warfighting units to 100%, the shortfall of skilled personnel able to meet this requirements has fallen into contractors hands.
- Total Outsourcing – This option is commonly referred to as the "keys to the kingdom" approach and is when the vendor is in total charge of a significant piece of the IS work.

An example of this is NASA's approach to shuttle mission operations. The contractor is responsible for the hardware, software and management of the entire operation. It is a combination of "body shop" and "project management" outsourcing. This option would enable all IS/IT functions to be contracted out. While the army has not elected this option yet, the growing sentiment is that information management functions are not core functions and the Army could save money and people "spaces" to be redistributed throughout the force by considering the outsourcing of all IS/IT functions.

While all of these options are feasible, the question that has not been answered is what are the potential implications for network centric warfare and the Army if the Army elects one or more of these options for its IT functions. Will outsourcing IT functions help or impair the Army as the Army moves into an era of network centric operations and from a legacy force to the objective force?

## IMPLICATIONS OF OUTSOURCING

The Army's mission is to fight and win our nation's wars. To accomplish this, the Army must have a force which is strategically responsive and dominant across the entire spectrum of military operations. The Army Vision calls for the force of the 21st century to be more responsive, deployable, agile, versatile, lethal, survivable, and sustainable. As stated earlier in this paper, network centric warfare is a key enabler for reaching this vision. NCW is the information superiority enabler that generates increased combat power by networking sensors, decision-makers, and shooters. But for NCW to work, the Army must have a secure, robust, deployable and reliable system of networks at every installation and unit across the globe. The networks must function in real-time and across branch and service boundaries. So the question that needs to be answered is: what are the potential implications if the Army elects to outsource functions supporting the GIG and NCW? This question can be broken down into three parts. What are the implications to warfigher, what are the implications to the Army's mission to maintain secure and robust networks and what are the implications to the Army's professional force structure?

### IMPLICATIONS TO THE WARFIGHTER

For the purpose of this analysis the term warfighter is used to describe any unit or element (combat, combat support or combat service support) which may be located within or deployed to a "combat zone" during hostilities. The question that will be considered is how will employing contractors in these units or on the battlefield effect a commanders ability to accomplish his mission. For the warfighter it can be assumed that the outsourcing options that could be

considered are limited to the body shop or project management options. Given this scenario there are many implications that could have an impact on the warfighter and his ability to accomplish his warfighting mission.

For a warfighting unit to be effective in the 21st century it must be responsive and deployable. The standard for the Interim Brigade Combat Team is that they can arrive anywhere in the world within 96 hours from the time they receive a deployment order. Current laws and requirements for deploying contract personnel may impact a unit's ability to rapidly deploy. Warfighting units are required to have every person within the unit complete the process for overseas movement upon arrival in the units. Medical screening, immunizations, wills and personal affairs and other administrative type functions are competed to ensure the soldiers are prepared to deploy. It is a relatively straightforward process for soldiers and units. However, with contractors, the situation is not so straightforward. Contractors cannot be required to undergo immunizations prior to deployment (unless specified in the contract). Updated medical records, dental records, passports, and next of kin notification – all need to be processed. If this is not accomplished prior to receiving a deployment order, the unit will be hard pressed to be ready to deploy the contractor. This situation is easily fixed by mandating that all contracts include this requirement be apart of the contract process. The unit can complete this process and be responsive but how does a unit ensure that a contractor will be permitted to enter the area of deployment?

By law, contractors must be approved to enter a country by the host government. Many people make the assumption that this will not be a problem because we are going there to help and all countries will just let the Army conduct is business. This is not always the case. Operation Joint Endeavor in Bosnia is a prime case in point. As US forces were preparing to move into Bosnia to support Operations Joint Endeavor, a logistics base was being established in Hungary to support the operation. The whole deployment operation of US forces was delayed a few days because the Hungarian government would not allow contractors to enter Hungary until their government received assurances that a portion of the contract work force would be Hungarian and that any non-Hungarian contractor would pay value-added taxes as well as Hungarian income taxes. Although this cost was simply applied to the contract and paid by the US government, the situation delayed the employment of the force.[18] How does the Army maintain deployable units under these constraints?

Another implication is the ability to sustain the force. If a commander has contractors within his unit, the commander is responsible for the sustainment of those personnel. Life support functions, facilities and equipment to work, distribution (mail, supplies, shipping of

goods), and transportation must all be accomplished by the unit to support the contractor. However, the Army builds a unit's Modified Table of Organization and Equipment (MTOE) based on the numbers and types of soldiers that are authorized a unit. The number of trucks or vehicles, the number of tents and cots, or numerous others things are based on the number of soldiers. Where does a commander get the assets needed to support contractors assigned to his unit? For every contractor assigned to a unit, this problem is just amplified.

Another implication for the warfighter is the requirement to protect contractors or in Army terms - survivability. Under the laws of land warfare, contractors are neither combatants nor noncombatants. They are called "civilians authorized to accompany the force." As such, they are entitled to some but not all of the protections afforded combatants and some, but not all, of the protections of noncombatants. In this status contractors are not permitted to bear arms unless in self-defense. A contractor is not permitted to participate in attacks on the enemy nor can they occupy defensive positions to secure a unit's perimeter. So these functions that are performed by soldiers cannot be performed by contractors. How would a Brigade TOC function if 25% of the functions within the TOC are performed by contractors? Who would be available to perform decision-making functions if the soldiers are all on guard duty? Another example of this dilemma can be seen when considering a unit deploying to an area that is under a nuclear, biological or chemical (NBC) threat. Commanders are responsible for ensuring that contractors are equipped and trained on NBC operations. This implies that the Army must train and equip the contractor against this threat. Again, MTOE's do not take contractors under consideration so the unit would be hard pressed to equip the contractors and generally speaking, most terms of a contract are written to only include the work that must be performed by the employee and do not cover training and protection issue.[19] The resolution of this problem would require additional money and force structure. This is contrary to the Army's goal of maintaining the current sized force structure.

Another implication that could effect the mission accomplishment of the warfighter is the level of commitment to the mission felt by the contractor. An advantage of using a contractor is that it allows military personnel to focus on warfighting while the civilian focuses on supporting functions. However, one basic difference between a soldier and contractor is the perceived dedication to the mission. Commanders who currently employ contractors sometimes feel that contractors either create unnecessary work to generate greater income for their company or that they only perform their duties to the exact limits of the contract. This has a tendency to create a "we-they" atmosphere which is detrimental to unit effectiveness. Any degradation to unit effectiveness adds risk to mission accomplishment and adds an increased threat to loss of life.

But this situation can easily be handled using effective leadership. But what if a contractor has a change of mind in the middle of a combat zone?

Implications of using IT contractors in war as we do in peace means that their services are mission essential. What if contractors choose to leave when a conflict occurs or intensifies? There are no legal guarantees to enforce a contractor to remain in a combat zone. Even if the terms of a contract calls for employees to stay during a conflict, and the company is held financially liable for that, an employee merely has to resign to relieve himself of that obligation.[20] There are two prime examples where a situation like this has occurred.

One example cited as an indication of how civilian support on the battlefield may work occurred in Korea in 1976. When the famous tree-cutting incident occurred in August 1976, the National Command Authority (NCA) was concerned that the situation would expand and potentially start another Korean War. To prepare for this potential scenario the NCA increased the alert status of all US forces to Defense Readiness Condition (DEFCON)-3. This condition indicates that the threat of war is likely. As a result of this increased DEFCON status, hundreds of Department of the Army civilians who had replaced military depot maintenance and supply workers in Korea requested immediate transportation out of Korea.[21]

Another incident cited occurred during the Gulf War. One primary contractor, fearing missile attacks against its employees, withdrew all its personnel from Saudi Arabia and returned them to the United States. The company alleged that the risk of death or injury to its employees outweighed the profit motive for the company. The employees left the war zone, the company paid the fine and the functions they were performing were left unattended until a replacement contractor could be found.[22] However, this act was not illegal.

Current laws state that contractors providing services designated as essential are expected to use all means at their disposal to continue to provide such services, in accordance with the terms and conditions of the contract, during periods of crisis until appropriately released or evacuated by military authority.[23] The company that supplies the contractor is responsible for ensuring their employees meet this requirement. However, if an employee simple quits the company, that individual is no longer required to meet the terms and conditions of the contract. Some contractor personnel interviewed said that their companies permit them to leave areas of potential hostilities at their own discretion and would be reassigned elsewhere in the company organization. In a survey conducted in Europe, 25 percent of the contract employees interviewed said they were not likely to remain in Europe if hostilities were to break out.[24]

The Army cannot overcome the problem of contractors leaving by requiring clauses that obligate the contractor to compensate for the unplanned departure of their personnel. It is not

unlawful for employees to leave a hostile area. In the absence of a formal declaration of war, there are no legal sanctions which can be imposed against civilians who leave overseas jobs without permission.[25] Overcoming this risk would require a change to the laws of the United States.

## IMPLICATIONS TO THE MISSION

The mission of outsourcing IT contractors in support of NCW would be to provide the Army with the capabilities to support the GIG and its components. To accomplish the goals of NCW, the GIG and its components must be dynamic, adaptable, flexible and secure. To fail in this would mean a failure of NCW. This failure would translate into a reduced effectiveness of the Army's ability to command and control, deploy, and sustain its forces and would put at risk the accomplishment of its wartime mission. The implied question is how could outsourcing IT functions potentially effect the Army's wartime mission.

The first implication of outsourcing IT functions is the potential increase in the "insider" threat risk. Most information security experts agree that "insiders" constitute the greatest threat to an organization. Since IT employees would have intimate knowledge of an organization's vulnerabilities and safeguards, it stands to reason that attacks from within would be far more devastating that those from the outside. Since a majority of the information passing over the GIG would be classified and contain many national secrets, access and ability to attack this information places the Army at a great potential risk if the personnel handling this information cannot be trusted. The Army ensures the trust of an individual is relatively secure by requiring them to receive security clearances. These personnel security measures are expensive and take time to complete. The Information Technology Association of America recently estimated a shortage of nearly 850,000 IT workers in the U.S. alone. With the demand so high and competition for these resources so stiff, few commercial organizations want to spend the time and money involved in undertaking even routine background checks. But in the IT world, this is extremely important. Psychological test of IT employees have identified a single predominant personality trait. The vast majority of IT employees tend to be introverts. Accordingly, many IT employees prefer to work independently, tend to resist authority, and worry less about the opinions and agendas of others. Also, previous research on introverts has indicated that they are more sensitive to environmental stress and less socially-skilled than extroverts. In practical terms, this means that IT employees are more likely to become stressed and disgruntled. Disgruntled employees are more likely to take actions that are detrimental to proper information flow or to sell our nation's secrets to an enemy force. While the quick answer to this problem is

to require the government to complete a security check on every employee, a major problem in DOD is the current backlog of background investigations. It is estimated that over 500,000 investigations on military and DOD civilian personnel are delinquent.[26] With DOD's backlog, the Army relies on contractors to complete an independent security check to supplement the Army's check. Requiring the Army to grant all contractors security clearances through its resources would result in many positions remaining unfilled for an extended period of time.

Another aspect of the "insider" threat concerns the companies that would bid on Army contracts in support of NCW . As stated earlier there is a large shortage of IT workers in the United States. To overcome this shortage companies need to go elsewhere. Technically minded immigrant labor, particularly from China, Pakistan, and India, will work for far less that US citizens when a potential green card is part of their employment package. Congress is being told by information systems giants like Intel and Microsoft that foreign IT workers quotas must be increased to assure a flow of new program and network administrators. [27] How does the Army evaluate a contract when a vast majority of a company's workforce are citizens of potential adversaries? How do you determine the threat from inside the company as employees discuss issues with their supervisors? Who handles the management functions and responsibilities?

There is also a new concern that is developing as our world becomes more "globalized." Outsourcing a critical function to a commercial enterprise puts at risk that function. An astute enemy could begin to attack the Army's institutional capabilities that are outsourced by acquiring control of those operations. It is not beyond the realm of possibility that an originally wholly owned subsidiary of a major defense contractor be bought out by a multinational corporation with questionable alliances. This cooperation could effect our mission in numerous ways. One example of how they could impact the Army's mission is to look at the communications component. Assume that we outsource our requirement to transmit data from one installation in the US to another installation in Germany. The company that supports this mission is owned by India. The same company owns and operates communication assets in Kosovo. This company in Kosovo is highly profitable and generates much more income than the US contract. Problems in Kosovo force the US to attack communication sites within Kosavo resulting in the loss of this Indian operational asset and revenue. In retaliation, the Indian government refuses to allow traffic to travel over its systems because they do not agree with the US's action. It may cost the Indian owned company some money, but what would be the impact do the Army forces trying to execute a critical mission? The primary motive of commercial enterprises is to make a profit. [28] How does the Army consider this potential as it looks to outsource all IT requirements?

IMPLICATIONS TO THE ARMY

If the sentiment throughout the Army remains to outsource all IT functions, what effect could this have on the Army? The main implication of taking this path is the impact on the profession of arms. An example of this is the career progression path for officers and NCOs. Over recent years most all logistic support functions have been conducted by contract personnel. With contractors responsible for supplies on the battlefield, there is no trained inter-Army force structure capable of handling this function. Gone are the problem-solving opportunities so critical in preparing senior logistics officers and NCOs. Gone are the hands-on training and real-world opportunities that gave most logisticians today the sound foundation to handle senior-level logistics decisions. Without this base and knowledge, how will the Army make informed critical decisions. If contractor support is implemented for most or all of the Army's current IT systems, where do senior communicators of the future get their professional development.[29] To reach the highest levels of management requires experiences from the grass roots level. How will the Army grow NCW leaders and managers and decision makers if all functions are turned over to outsourcing?

**CONCLUSION**

The evaluation of the implications associated with outsourcing IT functions within the Army is mute to some degree since the decision has already been made. Contractors are currently working and are deployed in units throughout the Army. The Army is developing doctrine to address the issues of contractors on the battlefield and to address other concerns of that nature. But what is important is the next step. How far should the Army go?

From the authors perspective, the Army would be at great risk if it determined to outsource all IT functions that support NCW. The Army cannot give up its management responsibilities and total ability to perform the functions of maintaining a secure, robust, deployable system of networks. It needs junior soldiers and officers performing these functions who will later grow into the leaders and managers of the future force. We need soldiers to which we trust with our lives and the security of our nation. To hand over these functions to a "job market" instead of a profession generates increased threats to the Army and its mission.

At the same time it is a reality that the Army does not have the resources to do the mission alone. The Army does not have the ability to fully man all IT functions with soldiers if it wants to maintain a viable warfighting force. Contractors and outsourcing are here to stay and may even be the "wave of the future" despite its inherent risks. However, risking responsibly means attempting to outmaneuver any threat to the risk's success.[30] This means making sound

and deliberate decisions to enhance the use of available military personnel and to reduce risk. In order to risk responsibly, we must proceed carefully, evaluating the second and third order effects of any decision we make. The way the Army proceeds with this critical decision can mean the difference in developing a force multiplier capability or a warfighting detractor. It could effect the Army's missions and tip the scales in favor of the enemy. That is unaffordable. Outsourcing just for the sake of conserving fiscal resources is the wrong approach. The Army can gain some fiscal savings and increased efficiencies through the outsourcing of IT requirements but the decision on what parts or components that should be outsourced should be based on the risk management decision process, not the dollar management decision process.

WORD COUNT =7884

## ENDNOTES

[1] J. Michael Brower, Outsourcing and Privatizing Information Technology: Re-examining the Savings [on-line] (Washington, D.C.: Department of Justice, Immigration, and Naturalization Service, 1999, accessed 11 September 2001); available from http://www.stsc.hill.af.mil/CrossTalk/1999/jan/brower.asp; Internet, 1-6.

[2] Vernon Loeb and Greg Schneider, NSA Picks Information Technology Contractor [on-line] (The Washington Post-Online, 2001, accessed 11 September 2001); available from http://www.washingtonpost.com/ac2/wp-dyn; Internet, 1-3.

[3] Peter Reif, Department of the Navy Information Systems and Technology Outsourcing Initiatives and the Insider Threat: A Cause for Concern [on-line] (SANS Institute, 2000, accessed 11 September 2001); available from http://www.sans.org/infosecFAQ/casestudies/navy.htm; Internet, 1-5.

[4] Director for Strategic Plans and Policy, J5; Strategy Division, Joint Vision 2020, (Washington, D.C.: U.S. Government Printing Office, June 2000), 15.

[5] David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition, (Washington, D.C.: CCRP Publication Series, February 2000), 88.

[6] Dennis Steele, "The Army Magazine Hooah Guide to Army Digitization," US Army War College Course 3: Joint Processes and Landpower Development, Volume I, (Carlisle Barracks, PA: U.S. Army War College, 18 October 2001), 341.

[7] Vice Admiral Arthur K. Cebrowski, "Network-centric Warfare: An Emerging Military Response to the Information Age," US Army War College Course 2: War, National Security Policy & Strategy, Volume IV, (Carlisle Barracks, PA: U.S. Army War College, 30 July 2001), 217.

[8] Joint Chiefs of Staff, The Joint Staff Officers Guide 2000, JFSC Pub 1, (Washington, D.C.: U.S. Joint Chiefs of Staff, 2000), 3-42.

[9] Ibid, 3-44 to 3-48.

[10] Department of the Army, United States Army 2001: Weapon Systems, (Washington. D.C.: U.S. Government Printing Office, 2001), 1.

[11] Ibid, 8-62.

[12] Ibid, 66-84.

[13] Ibid, 174.

[14] Department of Defense, Network Centric Warfare: Department of Defense Report to Congress, [on-line] (Washington, D.C.: 27 July 2001, accessed 8 December 2001); available from http://www.c3i.osd.mil/ncw/ncw-appendix.pdf; Internet, Appendix A.

[15] Katherine McIntire Peters, "Civilians at War," Government Executive, July 1996, 27.

[16] Stephen P. Ferris, "Outsourcing the Sinews of War: Contactor Logistics," Military Review, September-October 2001, 76.

[17] Mary C. Lacity and Rudy Hirschheim, Information Systems Outsourcing: Myths, Metaphors and Realities, (New York: John Wiley & Sons, 1993), 2.

[18] David L. Young, "Planning: The Key to Contractors on the Battlefield," Army Logistician, [on-line] (Washington, D.C.: 1999, accessed 20 November 2001); available from http://www.almc.army.mil/ALOG/issues/MayJun99/MS344.htm; Internet, 1-6.

[19] Joe A. Fortner, "Managing, Deploying, Sustaining, and Protecting Contractors on the Battlefield," Army Logistician, [on-line] (Washington, D.C.: 2000, accessed 20 November 2001); available from http://www.almc.army.mil/ALOG/issues/SepOct00/MS571.htm; Internet, 1-7.

[20] Captain Isolde K. Garcia-Perez, "Contractors on the Battlefield in the 21st Century," Army Logistician, [on-line] (Washington, D.C.: 1999, accessed 20 November 2001); available from http://www.almc.army.mil/ALOG/issues/NovDec99/MS454.htm; Internet, 1-6.

[21] Eric A. Orsini, "Contractors on the Battlefield: Risks on the Road Ahead," Army Logistician, [on-line] (Washington, D.C.: 1999, accessed 9 December 2001); available from http://www.almc.army.mil/ALOG/issues/JanFeb99/MS376.htm; Internet 1-5.

[22]Stephen P. Ferris, "Outsourcing the Sinews of War: Contactor Logistics," Military Review, September-October 2001, 76.

[23] Department of the Army, Assistant Secretary of the Army, Installation, Logistics, and Environment, SAIL-LOG, Information Paper, 23 October 1997.

[24] Ibid.

[25] Ibid.

[26] Peter Reif, Department of the Navy Information Systems and Technology Outsourcing Initiatives and the Insider Threat: A Cause for Concern [on-line] (SANS Institute, 2000, accessed 11 September 2001); available from http://www.sans.org/infosecFAQ/casestudies/navy.htm; Internet, 1-5.

[27] J. Michael Brower, Outsourcing and Privatizing Information Technology: Re-examining the Savings [on-line] (Washington, D.C.: Department of Justice, Immigration, and Naturalization Service, 1999, accessed 11 September 2001); available from http://www.stsc.hill.af.mil/CrossTalk/1999/jan/brower.asp; Internet, 1-6.

[28] James H. Ward, "Second Thoughts on Outsourcing for the Army," US Army War College Course 4: Implementing National Military Strategy, Volume II, (Carlisle Barracks, PA: U.S. Army War College, 19 November 2001), 14-20.

[29] Eric A. Orsini, "Contractors on the Battlefield: Risks on the Road Ahead," Army Logistician, [on-line] (Washington, D.C.: 1999, accessed 9 December 2001); available from http://www.almc.army.mil/ALOG/issues/JanFeb99/MS376.htm; Internet 1-5.

[30] Gene Calvert, Highwire Management: Risk Taking Tactics for Leaders, Innovators, and Trailblazers (San Francisco: Jossey-Bass, 1993), 152.

## BIBLIOGRAPHY


Alberts, Daivid S., Garska, John J., Stein, Fredrick P., Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, D.C.: CCRP Publication Series, February 2000.

Brower, J. Michael, Outsourcing and Privatizing Information Technology: Re-examining the Savings. Washington, D.C.: Department of Justice, Immigration, and Naturalization Services, January 1999. On-line. Available from http://www.stsc.hill.af.mil/CrossTalk/1999/jan/brower.asp.

Calvert, Gene. Highwire Management: Risk Taking Tactics for Leaders, Innovators, and Trailblazers. San Francisco: Jossey-Bass, 1993.

Captain Garcia-Perez, Isolde K. "Contractors on the Battlefield in the 21st Century". Army Logistician. 1999. On-Line. Available from http://www.almc.army.mil/alog/issues/NovDec99/MS454.htm.

Director for Strategic Plans and Policy, J5; Strategy Division, Joint Vision 2020. Washington, D.C.: Director for Strategic Plans and Policy, J5, June 2000.

Ferris, Stephen P., "Outsourcing the Sinews of War: Contractor Logistics". Military Review. Washington, D.C.: Department of the Army, September-October 2001.

Fortner, Joe A. "Managing, Deploying, Sustaining, and Protecting Contractors on the Battlefield". Army Logistician. 2000. On-Line. Available from http://www.almc.army.mil/ALOG/issues/SepOct/MS571.htm

Joint Chiefs of Staff, The Joint Staff Officers Guide 2000, JFSC Pub 1. Washington, D.C.: U.S. Joint Chiefs of Staff, 2000.

Lacity, Mary C. and Hirschheim, Rudy, Information Systems Outsourcing: Myths, Metaphors and Realities. New York: John Wiley & Sons, 1993.

Loeb, Vernon and Schneider, Greg, "NSA Picks Information Technology Contractor". The Washington Post-Online. New York, 2001. On-Line. Available from http://www.washingtonpost.com/ac2/wp-dyn.

Orsini, Eric A., "Contractors on the Battlefield: Risks on the Road Ahead". Army Logistician. 1999. On-Line. Available from http://www.almc.army.mil/alog/issues/JanFeb99/MS376.htm.

Peters, Katherine McIntire, "Civilians at War," Government Executive. Washington, D.C., July 1996.

Reif, Peter, "Department of the Navy Information Systems and Technology Outsourcing Initiatives and the Insider Threat: A Cause for Concern". Information Security Reading Room. SANS Institute, September 2000. On-Line. Available from http://www.sans.org/infosecFAQ/casestudies/navy.htm.